Department of Homeland Security Daily Open Source Infrastructure Report for 08 January 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- CNN reports security at the Port of Miami was tightened Sunday, January 7, after three people, two of them hidden inside a truck container, tried to enter the port illegally. (See item 11)
- The Associated Press reports a Frontier Airlines jet attempting to land Friday, January 5, at Denver International Airport came within 50 feet of a smaller charter plane that had inadvertently entered the runway. (See item 12)
- The Department of Homeland Security has released fiscal year 2007 grant guidance and application kits for five grant programs that will total roughly $1.7 billion in funding for state and local counterterrorism efforts. (See item 25)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *January 06, Associated Press* — **Bush picks new head of nuclear agency.** The White House said Friday, January 5, that President Bush has chosen a replacement for the man ousted as head of the government's nuclear weapons program in the wake of reports of embarrassing security breakdowns. Bush selected Thomas P. D'Agostino, who currently serves as deputy

administrator of defense programs at the National Nuclear Security Administration, to succeed Linton Brooks in the top job there on an acting basis. Energy Secretary Samuel Bodman had said Thursday that Brooks would resign within the month. Brooks was reprimanded in June for failing to report to Bodman the theft of computer files at an NNSA facility in Albuquerque, NM, that contained Social Security numbers and other data for 1,500 workers. Then in October hundreds of pages of classified weapons−related documents from the Los Alamos National Laboratory in New Mexico were found during a drug raid in the home of a woman who had worked at the lab. That security breakdown was especially troubling, a department inspector general's report said, because it came after tens of millions of dollars had been spent to upgrade cyber−security at Los Alamos.
DOE press release announcing the Administrator's departure:
http://www.energy.gov/news/4562.htm
Source: http://www.mercurynews.com/mld/mercurynews/news/politics/163 96096.htm

2. *January 06, Associated Press* — **Winds knock out power, topple trees in Los Angeles area.** A strong Pacific cold front moved across Southern California on Friday, January 5, scouring the region with powerful winds that downed power lines. At least 140,000 electrical customers in Los Angeles, coastal suburbs and inland cities to the east experienced outages of various lengths after the winds arrived in the early morning hours, and about 36,000 remained blacked out at midafternoon, utilities representatives said. At midafternoon, Southern California Edison said about 105,000 customers had had outages since about 2 a.m. PST and 4,000 were currently without power. Hardest−hit areas were close to the foothills of San Gabriel Valley and San Bernardino and Riverside counties. Outages also occurred in Orange County, Santa Monica Bay communities and Compton. Los Angeles had 32,000 customers without power at midafternoon. The total number of outages was not available, but Carol Tucker of the Los Angeles Department of Water and Power said that the most at any given time was about 35,000 or 36,000.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/163979 04.htm

3. *January 06, Washington Post* — **In the global energy rush, nuclear gets a resurgence.** Faced with evidence that coal− and oil−fired electric plants are overheating the planet, and alarmed by soaring demand for electricity, governments from South America to Asia are turning once again to a power source mostly shunned for two decades as too dangerous and too costly. Globally, 29 nuclear power plants are being built. Well over 100 more have been written into the development plans of governments for the next three decades. India and China each are rushing to build dozens of reactors. The United States and the countries of Western Europe, led by new nuclear champions, are reconsidering their cooled romance with atomic power. International agencies have come on board; even the Persian Gulf oil states have announced plans for nuclear generators. Utilities are dusting off plans for nuclear plants even though most of the problems that shelved those projects remain. The costs and time to build the concrete−encased plants far exceed those of conventional plants. There still is no safe permanent storage for used fuel. Added to these problems is the worry of a terrorist attack on a nuclear plant. Similar jitters about the reliability −− and price −− of traditional fuels are adding to the rush to nuclear.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/01 /05/AR2007010502191_pf.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *January 05, Associated Press* — **Ammonia leak prompts evacuations.** Ammonia leaking from a 7,500−pound tank at the Koch Food plant in Sylacauga, AL, forced evacuations Friday, January 5. Residents living within a half−mile radius of the plant on Merkel Avenue were evacuated.
   Source: http://gainesville.com/apps/pbcs.dll/article?AID=/20070105/A_PN/701054168

[Return to top]

Defense Industrial Base Sector

5. *January 05, Aviation Now* — **Air Force: National airspace security plan is on track.** The U.S. Air Force says its plan to prevent another terrorist attack using hijacked jets is on track, despite service auditors' comments that the program is over budget and behind schedule. The service plans to award another estimated $47 million in work by February for the Battle Control Systems, a national airspace security network charged with a variety of defense missions, including stopping drug smuggling. The initial contract for the first part of the program, called Battle Control System−Fixed, was worth about $30 million. But the cost of follow−on work is coming to more than three times that amount, and Air Force officials acknowledge that the final cost could be hundreds of millions of dollars. The service said this is all part of a "spiral development" acquisition plan which provides greater capability over a period of time with incremental cost increases.
   Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/AIR01057.xml

6. *January 05, Federal Computer Week* — **Counter−IED systems jam tactical comms in Iraq.** Jammers used by U.S. forces in Afghanistan and Iraq to defeat radio−controlled improvised electronic devices (IEDs) have the side effect of knocking out a wide range of tactical radio systems, according to the Naval Sea Systems Command. NAVSEA, which is asking for industry input on mitigating the problem, said IED jammers, known as Counter Radio Controlled Improvised Explosive Device Electronic Warfare (CREW) systems, can cause the “loss of all communications” from co−located or nearby tactical radio systems. The Navy manages the joint CREW program for Office of the Secretary of Defense’s Joint IED Defeat Organization. At the same time, active battlefield radio systems interfere with the IED jammers “to the extent that the CREW systems become ineffective,” according to NAVSEA's request for information. NAVSEA has asked industry to come up with an interference mitigation system that will enable simultaneous operations of IED jammers and tactical communications systems in the same location or vehicle.
   Source: http://www.fcw.com/article97264−01−05−07−Web

[Return to top]

Banking and Finance Sector

7. *January 15, BusinessWeek* — **Pitfalls of gift cards.** In the biggest year for gift cards ever, with annual sales rising seven percent, to $53 billion, according to researchers Mercator Advisory Group, buyers and receivers are learning the pitfalls of the prepaid cards issued by retailers. Fraud schemes generally fall into three basic types: stealing data such as bar codes and magnetic strip information, planting data, and indulging in checkout scams. Thieves may copy data off unsold cards, then use the store's Website or 800 number to check their status. Once the cards are bought and loaded with dollars, crooks use the data to buy goods online or to create bogus cards. Other scammers clone cards they own and plant the copies in stores to be sold. When the cards are activated, the money goes onto the thieves' cards. Employees may also pretend a card is empty or deactivated and persuade the customer to hand over the "worthless" card, hoping to use it later. They may just swap them, pocketing activated cards at the register while slipping customers look−alikes. Or they may clone cards using information off discarded receipts.
   Source: http://www.businessweek.com/magazine/content/07_03/b4017054. htm

8. *January 05, Finextra (UK)* — **Chip and PIN hacked; researchers get terminal to play Tetris.** Security researchers at the University of Cambridge in the UK have managed to hack a so−called tamper resistant Chip and PIN terminal and get it to play Tetris. Steven Murdoch and Saar Drimer got Tetris working by replacing most of the terminal's internal electronics. The hacking illustrates how scanners may be able to physically modify terminals. The researchers posted a video of the hack attack on YouTube. In a Web blog, the researchers say even a perfect tamper resistant terminal will only ensure that the device cannot communicate with a bank once opened. It does not prevent anyone from replacing a terminal's hardware and presenting it to customers as legitimate in order to collect card numbers and PINs.
   Source: http://finextra.com/fullstory.asp?id=16332

9. *January 05, Register (UK)* — **Google blacklist sheds light on phishing tactics.** An analysis of Google's blacklist of suspected phishing sites found that eBay, PayPal, and Bank of America together account for almost two in three (63 percent) of suspected scam sites. Security researcher Michael Sutton also discovered that Yahoo! hosts a significant number of bogus Websites −− as identified by Google's blacklist) −− that try to trick surfers into handing over Yahoo! login credentials. Information from the list is used by anti−phishing technology within the Firefox 2 browser and by the Google Toolbar for Firefox. Sutton found that 83 percent of sites detailed on the list are no longer available. By their nature, phishing Websites have a rapid turnover but Google's blacklist undoubtedly help CERTs and other net defenders to identify and remove bogus Websites more quickly. Most of the Websites contained in the list use social engineering techniques. Sutton found little evidence of sites that attempt to use software vulnerabilities to swipe passwords from surfers.
   Source: http://www.channelregister.co.uk/2007/01/05/google_phishing_ blacklist/

10. *January 05, Finextra (UK)* — **Bank of Queensland issues credit card to cat.** Australia's Bank of Queensland has apologized for issuing a credit card to a customer's cat after its owner decided to test the bank's identity screening system. The bank issued a credit card to Messiah the cat after its owner, Katherine Campbell from Melbourne, applied for a secondary card on her account under its name. Campbell told reporters that the bank requested identification from Messiah but later sent a credit card without receiving any proof of ID. And Campbell −− who is the primary credit card holder −− says she was not notified that a secondary credit card attached

to her account had been issued.
Source: http://finextra.com/fullstory.asp?id=16334

[Return to top]

Transportation and Border Security Sector

11. *January 07, CNN* — **Security high at Port of Miami after alleged entry attempt.** Security at the Port of Miami was tightened Sunday, January 7, after three people, two of them hidden inside a truck, allegedly tried to enter the port illegally, federal law enforcement sources said. The FBI said the three were being held on state charges. "The cargo area is closed for now while the FBI, Miami−Dade police, and Customs and Border Patrol search the truck container," said Port of Miami spokesperson Andrea Muniz. "The port side handling passengers remains open." Though the port as a whole remains open, cargo is not leaving the port while additional container searches are under way, a spokesperson for the Coast Guard said. Federal law enforcement sources described the three as being of Middle−Eastern descent. The driver was described as being of Iraqi descent and one of the other men appeared to be of Lebanese descent, the sources said. One of them was driving an 18−wheeler and was stopped at the entrance for not having the proper license to drive onto the property, FBI spokesperson Judy Orihuela told CNN. The driver also allegedly said he was alone in the truck. During the search, two other people were found in the cargo container, the FBI said.
Source: http://www.cnn.com/2007/US/01/07/miami.port/index.html

12. *January 06, Associated Press* — **Airliner nearly collides with charter jet in Denver.** A Frontier Airlines jet attempting to land Friday, January 5, at Denver International Airport came within 50 feet of a smaller charter plane that had inadvertently entered the runway, federal aviation officials said. The Frontier crew spotted the Key Lime Air plane in time, aborted the landing and continued flying until it could land the jetliner a short time later, authorities said. No injuries were reported. The National Transportation Safety Board (NTSB) and Federal Aviation Administration are investigating. The NTSB said the Frontier Airbus A−319 from St. Louis, MO, had emerged from low clouds as it was about to land about 7:30 a.m. MST when the flight crew saw the charter plane. It was snowing and misty at the time, with half−mile visibility, but NTSB spokesperson Ted Lopatkiewicz said there was no way to tell whether those conditions contributed to the incident.
Source: http://www.cnn.com/2007/US/01/05/close.call.ap/index.html

13. *January 06, Washington Post* — **Colorado avalanche buries highway.** An avalanche roared across a mountain highway on the Continental Divide on Saturday morning, January 6, sweeping two cars off the road near Berthoud Pass, CO, onto a steep downward slope but causing only one serious injury. People from nearby cars dug frantically into the instant mound of snow and debris on the road to free the eight passengers in the two cars that were hit, police said. The cascade of snow, rocks and trees that came rushing down the side of Stanley Mountain about 10:30 a.m. MST covered all three lanes of U.S. 40. The road is a key thoroughfare linking Denver and Interstate 70 with the ski resorts of Winter Park and Steamboat Spring "We have recovered two vehicles that were driven over the edge of the highway," said Colorado State Patrol spokesperson Eric Wynn. The state patrol said eight people were taken to hospitals, but the worst injury incurred was apparently a broken leg. The

pass was reopened to traffic Saturday night. Unlike Denver, about 50 miles to the east, the Berthoud Pass area has not had unusually heavy snowfall so far this winter. Still, weather conditions have been conducive to an avalanche, according to the Colorado Avalanche Information Center.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/01/06/AR2007010600552.html

14. *January 05, Arizona Daily Star* — **Minutemen heading to back up National Guard.** Volunteers with the Minuteman Civil Defense Corps headed for the Arizona−Mexico border Friday, January 5, to provide backup for National Guard troops in response to an incident near Sasabe, AZ, in which the approach of armed men forced soldiers to retreat. About 11 p.m. Wednesday, soldiers with a National Guard Entry Identification Team saw a group of armed individuals approaching them in the desert, said Mario Martinez, spokesperson for the U.S. Customs and Border Protection's Border Patrol Office. The individuals came within 100 yards of the National Guard post, so the troops moved to a safer location and notified Border Patrol agents, Martinez said. When agents responded minutes later, the armed individuals were gone but the agents tracked their footprints to the U.S.−Mexico border, Martinez said. The incident occurred in the west desert corridor between Nogales and Lukeville near Sasabe, which has been a busy area for marijuana seizures since last year. Still, the Border Patrol does not know who the individuals were; why they were armed; or why they were in the United States, Martinez said. There was no verbal or physical confrontation between them and the guard troops, he said.
Source: http://www.azstarnet.com/sn/hourlyupdate/163418

15. *January 04, Washington Post* — **Immigrant processors fall behind.** As the White House and Congress prepare to overhaul the nation's immigration laws, U.S. officials have concluded that they lack the technology and resources to handle the millions of applications for legal residency that could result from the changes and that several efforts to modernize computers have gone astray. Immigration officials have said for years that it is critical to update an antiquated, paper−based application process before the government grants a new path to citizenship for as many as 12 million illegal immigrants living in the United States or creates a temporary−worker program, as senators and the Bush administration propose. But in recent months, U.S. Citizenship and Immigration Services (USCIS) officials have determined that the troubled, $2−billion−a−year agency is unable to effectively manage its existing work, much less a flood of new applications. A report released December 20 by Department of Homeland Security Inspector General Richard L. Skinner cited a long list of setbacks and concurred with internal USCIS reviews that the bureau "lacks the processing capacity, systems integration and project management resources needed to manage a potential increase in workloads.
Review of U.S. Immigration and Customs Enforcement's Detainee Tracking Process, OIG−07−08: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07−08_Nov06.pdf
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/01/03/AR2007010301618.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

16. *January 05, USAgNet* — **Colorado blizzard could set record for livestock deaths.** Colorado Agriculture Commissioner Don Ament says he expects the recent blizzard that hit the state will be a crueler killer than a 1997 storm that claimed 30,000 heads of livestock in the same region. Ament said the storm would likely kill at least 40,000 head of livestock in southeastern Colorado, an area home to more than 300,000 farm animals. It's been a week since the blizzard dumped three feet of snow on the region and kicked up 15−foot−tall snowdrifts, effectively suffocating some animals and stranding others, thereby depriving them of feed and water. Ament expressed concern over reports from farmers who have lost as many as 1,500 cattle to suffocation, and thousands of hogs to building collapses.
Source: http://www.usagnet.com/story−national.php?Id=39&yr=2007

17. *January 02, Ohio State University Center for Diagnostic Assays* — **Center develops assay for detecting very virulent Infectious Bursal Disease Virus.** The Ohio State University Center for Diagnostic Assays announces a significant diagnostic discovery. Animal Health Scientist, Daral Jackwood, has developed a validated real−time PCR Assay for the rapid detection of nucleotide sequences that are unique to very virulent Infectious Bursal Disease Virus (vvIBDV) strains affecting the poultry industry. This new assay distinguishes vvIBDV strains from non−vvIBDV classic and variant strains. Due to the ever−increasing worldwide trade of chicks and hatching eggs, there is a real and immediate concern that the vvIBDV will continue to spread, causing dramatic losses on every continent including North America. In 2004 alone, over 18 million chicks and nine million poultry hatching eggs were imported into the U.S. Said Jackwood, “Until now, no validated rapid assay for the detection of all known vvIBDV strains existed. In countries with vvIBDV, this assay is necessary for the effective monitoring and control of this devastating disease. In countries without the virus, the assay would be a first line of defense needed to prevent vvIBDV from entering domestic poultry operations.
IBDV information: http://www.oardc.ohio−state.edu/ibdv/
Source: http://www.oardc.ohio−state.edu/cda/newsrelease.asp

[Return to top]

Food Sector

18. *January 05, Food Safety and Inspection Service* — **Sausage products recalled.** Gold Star Sausage Co., Inc, a Denver, CO, firm, is voluntarily recalling approximately 15,514 pounds of sausage products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Friday January 5. The sausage products were distributed to retail and institutional establishments in Alabama, Colorado, Florida, Georgia, Idaho, Indiana, Iowa, Louisiana, Massachusetts, Michigan, Minnesota, Mississippi, New Jersey, New Mexico, Pennsylvania, South Carolina, Tennessee and Utah. The problem was discovered through microbiological testing completed by a non−government laboratory. FSIS has received no reports of illnesses associated with

consumption of this product. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_002_2007_Relea se/index.asp

[Return to top]

Water Sector

19. *January 03, Bloomberg* — **Bird flu viruses unlikely to endure water treatment.** Bird flu viruses are unlikely to survive sewerage and drinking water treatment systems, making it doubtful contaminated feces could infect plant workers and spread through tap water, scientists at Cornell University said. The researchers studied a low−pathogenic H5N2 avian influenza virus, which they said resembles the lethal H5N1 strain circulating in Asia and Africa. Water treatments, including chlorination, ultraviolet radiation and bacterial digesters killed the microbes, said Araceli Lucio−Forster, a microbiologist at Cornell. The finding may reduce concerns about drinking water as a mode of infection during a pandemic. "You have some 50,000 treatment plants in the U.S., and all these operators that run the plants were concerned that if there were an influenza outbreak and everyone were sick, is it going to come into the plant and infect them and others?" Dwight Bowman, a professor of parasitology at Cornell, said Tuesday, January 2.
Source: http://www.bloomberg.com/apps/news?pid=20601103&sid=awkOSNqi viT8&refer=us

[Return to top]

Public Health Sector

20. *January 07, Bloomberg* — **Indonesia confirms 75th case of human bird flu infection.** A 14−year−old boy tested positive for bird flu in Indonesia, marking the country's first case in almost two months and its 75th overall, a Health Ministry official said. The boy is being treated at Persahabatan Hospital in Jakarta after showing flu−like symptoms on January 1, Muhammad Nadirin, an official at the Health Ministry's avian flu information center, said Sunday, January 7. "We received a report that he had contact with a dead duck," Nadirin said. "We're launching a full investigation in his neighborhood in west Jakarta."
Source: http://www.bloomberg.com/apps/news?pid=20601080&sid=aj3xjU5j KCe0&refer=asia

21. *January 06, Agence France−Presse* — **Dead bird in Hong Kong tests positive for H5N1 virus.** A wild bird found dead in Hong Kong was infected with the fatal H5N1 strain of bird flu, the government has confirmed. The bird −− from a local species called the scaly−breasted munia −− was discovered in the busy shopping area of Causeway Bay on December 31. It was the only one of six dead birds found that tested positive for the deadly virus, the Agriculture, Fisheries and Conservation Department said on Saturday, January 6. Department officials have said winter was the migratory bird season, posing higher risks of bird flu.
Source: http://news.yahoo.com/s/afp/20070106/wl_afp/healthfluhongkon g_070106151108

22.

January 04, U.S. Health and Human Services — **HHS pursues advance development of new influenza antiviral drug.** U.S. Health and Human Services (HHS) Secretary Mike Leavitt announced Thursday, January 4, that HHS has awarded a $102.6 million, four−year contract for advanced development of their influenza antiviral drug, peramivir. In laboratory studies to date, peramivir has shown effectiveness against a number of influenza strains. Funding provided under the new contract will support further studies to determine if peramivir can be an effective treatment for seasonal and life−threatening influenza, including highly pathogenic H5N1 influenza. Additional research may also examine the drug's potential use for prophylaxis to protect against influenza infection. Funding in this contract will support manufacturing of clinical investigational and consistency lots; Phase 2 and 3 clinical studies to support product approval in the U.S.; manufacturing process validation; and other product approval requirements.
Source: http://www.hhs.gov/news/press/2007pres/20070104.html

23. *January 04, Journal of Infectious Diseases* — **Anthrax attack posed greater potential threat than thought.** A new study shows that more people were at risk of anthrax infection in the October 2001 attack on U.S. Senator Tom Daschle's office than previously known. On the other hand, the study shows, prompt intervention with antibiotics and vaccination appeared to be highly effective against the disease. In October of 2001, a letter containing spores of Bacillus anthracis, the bacterium that causes anthrax disease, was opened in Daschle's office at the Hart Senate Office Building in Washington, DC. Those in or near Daschle's office, judged likely to have been exposed to the spores, received antibiotics or a vaccine, as did others within or outside the building, and no deaths resulted from this act of bioterrorism. According to the new study of the event, however, people in areas assumed to be at minimal risk of exposure showed immune responses suggesting they had been exposed. Immune responses occurred not only in subjects in or near the Daschle office but also in those elsewhere in the Hart building, or even outside the building; the extent of exposure was thus greater than predicted.
Source: http://www.idsociety.org/Template.cfm?Section=News_from_the_Journals&CONTENTID=17799&TEMPLATE=/ContentManagement/Content Display.cfm

24. *December 21, Clinical Infectious Diseases* — **Prediction markets accurately forecast influenza activity.** Influenza experts have borrowed a page from economists, creating a futures market for influenza activity. In a prediction market, people with information about a future event buy and sell shares based on what they believe the likelihood of that event will be. "Health care workers possess current information that could be used to predict future infectious disease trends," explains Philip Polgreen, of the University of Iowa. But there is no mechanism to gather that data and digest it quickly enough to make it useful. "Prediction markets provide a way to collect and analyze information in real time," Polgreen says. Researchers set up a "flu market" for the 2004−05 influenza season in the state of Iowa. Sixty−one health care workers from a variety of backgrounds participated. The traders bought and sold shares based on the level of influenza activity in Iowa as reported by the Centers for Disease Control and Prevention's five−level grading system. The market accurately predicted the activity levels at the end of a target week 71 percent of the time, and was within one level 93 percent of the time. Longer−term predictions were less accurate, but still beat predictions based solely on historical averages up to four weeks in advance.
Source: http://www.idsociety.org/Template.cfm?Section=Home&CONTENTID=17644&TEMPLATE=/ContentManagement/ContentDisplay.cfm

[Return to top]

Government Sector

25. *January 05, Department of Homeland Security* — **DHS announces $1.7 billion available for local programs.** The Department of Homeland Security (DHS) released on Friday, January 5, fiscal year 2007 grant guidance and application kits for five grant programs that will total roughly $1.7 billion in funding for state and local counterterrorism efforts. With the fiscal year 2007 funding, the department will have invested nearly $20 billion in local planning, organization, equipment, training, and exercises. “DHS Secretary Michael Chertoff said, “The funds will be distributed to reduce risk across the United States, not just in a handful of places. But, let me be clear that the communities facing the highest risk will receive the majority of the funds.” The five programs that comprise the Homeland Security Grant Program encourage a regional approach to strengthening homeland security. Grant funding priorities include reducing risks of improvised explosive devices and radiological, chemical and biological weapons.
Remarks by Secretary Michael Chertoff:
http://www.dhs.gov/xnews/releases/pr_1168039350894.shtm
Report: http://www.dhs.gov/xlibrary/assets/grants−2007−program−overv iew−010507.pdf
Source: http://www.dhs.gov/xnews/releases/pr_1168010425128.shtm

[Return to top]

Emergency Services Sector

26. *January 05, Federal Computer Week* — **Despite improvements, FEMA's IT still needs work, IG says.** The Federal Emergency Management Agency (FEMA) has made progress on upgrading its pre−Hurricane Katrina information technology infrastructure but still faces challenges to long−term improvement, according to the Department of Homeland Security’s inspector general (IG). After an audit it performed in September 2005, the IG’s most recent report notes that funding and personnel constraints had forced FEMA to focus on short−term improvements ahead of the 2006 hurricane season.
IG Report: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07−17_Dec06.pdf
Source: http://www.fcw.com/article97260−01−05−07−Web

27. *January 05, Des Moines Register (IA)* — **Iowa emergency system remains a patchwork.** Iowa has improved the ability of its emergency agencies to communicate during disasters, but more work is needed to fix a "patchwork quilt" communications system, said Iowa Homeland Security Administrator David Miller. Statewide, it's difficult to rate Iowa's emergency communications interoperability, Miller said. Iowa's law enforcement, fire, emergency medical and emergency management communities have worked on communications issues for decades, he said, but some of the equipment is becoming old, and there are technical issues involving compatibility of networks. "In many places in the state, it is antiquated equipment. In other places, it is not just antiquated, but it lacks areas of coverage, and in some places we have just never had enough radios and equipment, especially for volunteer fire departments and some of the first−responder agencies," Miller said.

Source: http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20070105/NEWS10/701050368/1011

28. *January 05, Las Vegas Review−Journal* — **Las Vegas again deemed high−risk.** Las Vegas has again been placed on the Department of Homeland Security's list of high−risk targets for terrorist attacks, making it eligible for millions more in federal anti−terrorism dollars. State and federal officials announced Thursday, January 4, that they had met with Department of Homeland Security Secretary Michael Chertoff and secured the metropolitan area's designation as a high−risk area after it was downgraded last January. It is now eligible to get a chunk of the more than $700 million in homeland security funding. Although the Las Vegas metropolitan area was taken off the list of high−risk cities last year, it never lost funding. Jim O'Brien, the county's director of emergency management and homeland security, said Clark County received $7.7 million through the homeland security grant in 2006. In 2005, Clark County received $8.5 million through the same grant. O'Brien said funding would have been cut if the area was considered a lesser terrorist target for two years running.
Source: http://www.reviewjournal.com/lvrj_home/2007/Jan−05−Fri−2007/news/11801083.html

[Return to top]

Information Technology and Telecommunications Sector

29. *January 05, Reuters* — **Chinese Web users lose 10,000 domain names in quakes.** Chinese Web users lost around 10,000 Internet domain names due to disruption caused by last month's earthquakes off Taiwan, state media said on Friday, January 5. The domain names −− or Website addresses −− vanished after Chinese users were unable to update them or failed to re−register them on their expiry, the official Xinhua news service said, citing China International Network Information Center.
Source: http://news.yahoo.com/s/nm/20070105/wr_nm/china_earthquake_domain_dc

30. *January 05, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA07−005A: Apple QuickTime RTSP buffer overflow.** A vulnerability exists in the way Apple QuickTime handles specially crafted Real Time Streaming Protocol (RTSP) URL strings. Public exploit code is available that demonstrates how opening a .QTL file triggers the buffer overflow. However, US−CERT has confirmed that other attack vectors for the vulnerability also exist. Possible attack vectors include: 1) A Webpage that uses the QuickTime plug−in or ActiveX control; 2) A Webpage that uses the rtsp:// protocol; 3) A file that is associated with the QuickTime Player. Note that this vulnerability affects QuickTime on Microsoft Windows and Apple Mac platforms. Although Webpages can be used as attack vectors, this vulnerability is not dependent on the specific Web browser that is used. Apple iTunes and other software using the vulnerable QuickTime components are also affected. Solution: US−CERT is currently unaware of a solution to this problem. Until a solution becomes available, the workarounds provided in US−CERT Vulnerability Note VU#442497 are strongly encouraged: http://www.kb.cert.org/vuls/id/442497
Source: http://www.uscert.gov/cas/techalerts/TA07−005A.html

31. *January 04, eWeek* — **Patch Tuesday: Critical MS Office fixes coming.** Microsoft's security response team has announced plans to release eight security bulletins Tuesday, January 9, with patches for a slew of Windows and Office vulnerabilities. Four of the bulletins will deal directly with the Microsoft Office desktop suite, which includes the Microsoft Word software that has been the target of zero−day malware attacks. As part of its advance notification process, Microsoft said at least three of the four Office updates will be rated "critical," its highest severity rating.
Source: http://www.eweek.com/article2/0,1895,2079123,00.asp

32. *January 04, InfoWorld* — **Cisco warns of vulnerabilities in NAC product.** Networking equipment vendor Cisco Systems Inc. issued an advisory to customers Wednesday, January 3, about two serious vulnerabilities in its Cisco Clean Access software, a network access control product. The two issues could allow remote attackers to gain control of the devices, or glean sensitive data from Clean Access customers that could be used to compromise the Clean Access Manager (CAM) product, the company said. According to Cisco Security Advisory 72379, a problem with initial setup of the Cisco Clean Access Manager (CAM) and Clean Access Server (CAS) product makes it impossible to properly configure a "shared secret" that is used to authentication communications between the two devices. Remote hackers could take advantage of the vulnerability by establishing a TCP connection to the CAS device, Cisco said. A second vulnerability in the Clean Access Manager allows malicious users to view backups of the CAM database without first authenticating on the CAM device. A flaw in the way database backups are stored makes it possible to guess the backup file name and download it without authenticating, Cisco said.
Source: http://www.infoworld.com/article/07/01/04/HNciscoclean_1.htm l

33. *January 04, CNET News* — **PDF security risk greater than originally thought.** A recently discovered security weakness in the widely used Acrobat Reader software could put Internet users at more risk than previously thought, experts warned Thursday, January 4. Initially, security professionals thought that the problem was restricted and exposed only Web−related data or could support phishing scams. Now it has been discovered that miscreants could exploit the problem to access all information on a victim's hard disk drive, said Web security specialists at WhiteHat Security and SPI Dynamics. Key to increased access is where hostile links point. When the issue was first discovered, experts warned of links with malicious JavaScript to PDF files hosted on Websites. While risky, this actually limits the attacker's access to a PC. It has now been discovered that those limits can be removed by directing a malicious link to a PDF file on a victim's PC. "This means any JavaScript can access the user's local machine," said Billy Hoffman, lead engineer at SPI Dynamics. "Depending on the browser, this means the JavaScript can read the user's files, delete them, execute programs, send the contents to the attacker, et cetera. This is much worse than an attack in the remote zone."
Source: http://news.com.com/PDF+security+risk+greater+than+originall y+thought/2100−1002_3−6147428.html?tag=nefd.top

34. *January 04, IDG News Service* — **Patch issued for OpenOffice.org WMF vulnerability.** A patch has been released for a vulnerability in the OpenOffice.org productivity suite, a problem rated as "highly critical" by one security vendor. The flaw could be exploited by creating a malicious file in the Windows Metafile (WMF) or Enhanced Metafile formats. If the file was opened by a user, it could start running unauthorized code on a computer, according to an

advisory by Linux distribution vendor Red Hat Inc., which offers the OpenOffice suite with several of its products. OpenOffice.org has published a patch, which in turn is being distributed by Red Hat. The problem was first reported in October, but the vendors that distribute OpenOffice and often work together on security issues chose not to issue the patch until OpenOffice.org acknowledged earlier this week that it was a security issue, said Mark Cox, director of Red Hat's Security Response Team. No public exploits or even proof−of−concept code has been discovered, he added.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9007101&source=rss_topic85

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	6881 (bittorrent), 4662 (eDonkey2000), 1026 (win−rpc), 21165 (−−−), 25 (smtp), 445 (microsoft−ds), 57715 (−−−), 135 (epmap), 44556 (−−−), 27503 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer